

# Sequential Quantum Secret Sharing in a Noisy Environment aided with Weak Measurements

M. Ray,<sup>1</sup> S. Chatterjee,<sup>1</sup> and I. Chakrabarty<sup>2</sup>

<sup>1</sup>*Centre for Computational Natural Sciences and Bioinformatics,*

<sup>2</sup>*Center for Security Theory and Algorithmic Research*

*International Institute of Information Technology,  
Gachibowli, Hyderabad-500032, Andhra Pradesh, India.*

In this work we give a  $(n, n)$ -threshold protocol for sequential secret sharing of quantum information for the first time. By sequential secret sharing we refer to a situation where the dealer is not having all the secrets at the same time, at the beginning of the protocol; however if the dealer wishes to share secrets at subsequent phases she/he can realize it with the help of our protocol. First of all we present our protocol for three parties and later we generalize it for the situation where we have  $(n > 3)$  parties. Further in a much more realistic situation, we consider the sharing of qubits through two kinds of noisy channels, namely the phase damping channel (PDC) and the amplitude damping channel (ADC). When we carry out the sequential secret sharing in the presence of noise we observe that the fidelity of secret sharing at the  $k^{th}$  iteration is independent of the effect of noise at the  $(k - 1)^{th}$  iteration. In case of ADC we have seen that the average fidelity of secret sharing drops down to  $\frac{1}{2}$  which is equivalent to a random guess of the quantum secret. Interestingly, we find that by applying weak measurements one can enhance the average fidelity. This increase of the average fidelity can be achieved with certain trade off with the success probability of the weak measurements.

PACS numbers:

## INTRODUCTION

For a long time quantum entanglement ("spooky action at a distance") [1] was only of philosophical interest until people had found out various ways of utilizing it as a resource for information processing protocols like quantum teleportation [2], quantum super-dense coding, entanglement broadcasting and quantum cryptography [3, 4].

In quantum cryptography when we work with quantum systems, entanglement proves to be a useful resource in carrying out various protocols. Quantum secret sharing is no exception to it. In a nut shell, secret sharing refers to a situation where the sender shares a secret message between other parties in such a way that none of them can reveal the secret without the collaboration of others.

In quantum secret sharing (QSS) [4, 5] generally we deal with the problem of sharing of both classical as well as quantum secrets. This is done by using quantum resources like entangled states; mostly pure entangled state. These protocols include various attempts on tightening the security in presence of eaves droppers. It is not necessary that we always require three qubit entangled state as a resource for the most simplest secret sharing protocols. Karlsson et.al.[6] showed that similar quantum secret sharing protocols using bipartite pure entangled states also exist. However in general research was carried out mainly investigating the concept of quantum secret sharing using tripartite pure entangled states and multipartite states like graph states [7, 8, 9, 17, 18, 19, 20] as resources. More precisely when we talk about multi-qubit secret sharing, we generally talk about a situation

where the dealer wants to send multiple secrets; is a QSS scheme to various reconstructors. Apart from classical and quantum secret sharing, protocols have been given to share semi-quantum secrets using entangled states as the resource [21].

Recently in the reference [22], it was shown that quantum secret sharing is possible even with bipartite two qubit mixed states formed due to the transmission of qubits through noisy environment. In a realistic situation, the secret sharing of classical or quantum information will involve the transmission of qubits through noisy environment. As a result of which the resource state will become a mixed-state and the secret sharing will no longer be a deterministic one. In reference [23], authors proposed a protocol for secret sharing of classical information in the presence of such noise. In different works like [24, 25, 26, 27], it has been shown that quantum secret sharing is not only a mere theoretical concept, but also an experimental possibility.

In another piece of work authors have investigated the revocation of quantum secret back to the dealer and routing quantum information to different receivers in a network [28]. In the long run quantum secret sharing is also an important area to study in various quantum networks (QNet) as in recent times researchers have seen that both classical as well as quantum information can be transferred elegantly through quantum networks [29].

It is quite well-known that environmental interactions incurring loss of fidelity of the shared secret is an ubiquitous process and unless controlled using well-formulated schemes can reduce a shared secret in a pure state to one in maximally mixed state during the reconstruction

phase. Hence it becomes imperative to devise schemes of improving the fidelity of shared secret. In references [10, 11, 12, 13], authors have suggested that one can apply weak measurements [16] to protect the fidelity of quantum states subjected to decoherence through an amplitude damping channel (ADC) and this technique is even shown to be practically implementable. Recently in [14], authors have shown how efficiently one can employ the technique of weak measurement with post selection and its reversal to improve the fidelity of teleportation through an ADC. They also show how to exploit the power of post selection [16] in weak measurements to work with sub-ensemble of the initial states and hence reduce the suppression of decoherence of the transmitted qubits.

In this work we have given a protocol for sequential multi qubit secret sharing. This sequential secret sharing is useful when the dealer is not having all the secrets at the beginning of the protocol and wishes to send the secrets at subsequent stages. By our protocol one can achieve sequential secret sharing. We have also considered a realistic situation when the qubits are transferred from the dealer to other parties through noisy quantum channel. In that case we have seen that the fidelity of secret sharing at the  $k^{th}$  iteration is independent of the effect of noise at the  $(k - 1)^{th}$  iteration. Finally we employ the technique of weak measurement with post selection and its reversal to improve the fidelity of the shared secret under the effect of ADC. For any given input state parameters and strength of decoherence channel, we find out for what values of strength parameters of weak measurement and reverse weak measurement will help one to gain maximum fidelity of reconstructing the shared secret. We also show how the success probability of such an improvement technique decreases with increase in strength of weak measurement and that of the decoherence channel.

## QUANTUM SEQUENTIAL SECRET SHARING IN THE ABSENCE OF NOISE

In this section, we present a protocol by which Alice (the dealer) will securely share the secrets  $\psi_1, \psi_2, \dots, \psi_m$  among  $n$  parties at various stages of the protocol. By this we refer to a situation where the dealer is not having all the secrets at the beginning of the protocol. So he/she shares them at subsequent stages depending on the availability of the secrets.

### Sequential Secret Sharing with three Parties

In this subsection we begin with three parties, where Alice is the dealer and Bob and Charlie are the receivers. Alice wants to share the secrets  $|\psi_i\rangle = \alpha_i|0\rangle_1 + \beta_i|1\rangle_1$ ,

(where  $|\alpha_i|^2 + |\beta_i|^2 = 1$  and  $i$  is from 1 to  $m$ ) at the  $i^{th}$  iteration of the protocol, to both Bob and Charlie. However to do so Alice needs to share a quantum resource with the other two parties. In order to prepare this resource state Alice starts with a Bell state, say  $|\phi^+\rangle = \frac{1}{\sqrt{2}}\{|00\rangle_{23} + |11\rangle_{23}\}$ . The combined system of the Bell state and the secret  $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ , available to her at the first iteration is given by,

$$|\psi_1\rangle|\phi^+\rangle = \frac{1}{\sqrt{2}}(\alpha_1|000\rangle_{123}) + \frac{1}{\sqrt{2}}(\alpha_1|011\rangle_{123} + \alpha_1|100\rangle_{123} + \alpha_1|111\rangle_{123}). \quad (1)$$

Now Alice carries out a XOR operation between qubits 1 and 2 to obtain the three qubit entangled state

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}(\alpha_1|000\rangle_{123} + \alpha_1|011\rangle_{123} + \beta_1|110\rangle_{123} + \beta_1|101\rangle_{123}). \quad (2)$$

Then Alice keeps the qubit 2 with herself and sends the remaining qubits 1 and 3 to Charlie and Bob respectively. Here we consider the transfer of qubits to take place in an idealistic situation where the medium of transfer is free of noise. The three qubit entangled state shared between them can be re-written as

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}[|0\rangle_2\{|+\rangle_1(\alpha_1|0\rangle_3 + \beta_1|1\rangle_3) + |-\rangle_1(\alpha_1|0\rangle_3 - \beta_1|1\rangle_3)\} + |1\rangle_2\{|+\rangle_1(\alpha_1|1\rangle_3 + \beta_1|0\rangle_3) + |-\rangle_1(\alpha_1|1\rangle_3 - \beta_1|0\rangle_3)\}]. \quad (3)$$

After that Alice measures her qubit in the computational basis  $\{|0\rangle, |1\rangle\}$  and Charlie measures his qubit in  $\{|+\rangle, |-\rangle\}$  basis. At this point, Alice does not tell either Bob or Charlie about her measurement outcomes. This implies that the single-qubit density matrices of both Bob's and Charlie's qubits are  $(1/2)I$ , where  $I$  is the  $2 \times 2$  identity matrix. Thus at this stage of the protocol neither Bob nor Charlie has any information about Alice's qubit. Unlike other protocols, it is interesting to note that in our protocol we are carrying out single qubit measurements at two different locations instead of two qubit Bell measurement. Once the measurement is over from Alice's side the secret is shared between other two parties, Bob and Charlie. However neither of them can reveal the secret without the collaboration of the other party. This completes the sharing of Alice's secret. Now if Bob wants to reveal the secret, then both Alice and Charlie have to send their measurement outcomes to Bob in form of one classical bit. Depending on the outcomes of Charlie and Alice, Bob can reveal the secret by applying appropriate set of unitary transformations. This set of unitary transformations is shown in the following (TABLE I).

However if Alice wishes to carry out further secret sharing, Charlie needs to send his qubit to Alice. On receiving

TABLE I: Sharing of quantum secrets

Outcomes of Alice and Charlie	Unitary Transformations
$ 0\rangle,  +\rangle$	$I$
$ 0\rangle,  -\rangle$	$\sigma_z$
$ 1\rangle,  +\rangle$	$\sigma_x$
$ 1\rangle,  -\rangle$	$-i\sigma_y$

the qubit from Charlie, Alice applies the unitary transformation to convert it into  $|0\rangle$  state. In addition to that at each iteration Alice needs the state  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . With this single qubit state and the state obtained from Charlie she applies XOR operation to re-create a Bell pair  $|\phi^+\rangle = \frac{1}{\sqrt{2}}\{|00\rangle_{23} + |11\rangle_{23}\}$ . Then she follows the same steps to carry out further secret sharing. The key point of the protocol is that in order to carry out sequential secret sharing, at the end of each iteration Alice needs the supply of the qubit  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  along with the qubit transferred by Charlie.

### Sequential Secret Sharing with Multi-parties

In this subsection, we extend our protocol for a situation where we have more than three parties and consider a much more generalized condition having  $n$  parties other than the dealer herself. The protocol for multi party secret sharing is mainly a natural extension of our protocol for three parties. However the resource state required for secret sharing in this case is an  $n+1$  qubit pure entangled state given by,

$$|\Psi_{in}^{n+1}\rangle = \frac{1}{\sqrt{2}}(\alpha_i|000\dots 0\rangle_{123\dots(n+1)} + \alpha_i|011\dots 1\rangle_{123\dots(n+1)} + \beta_i|110\dots 0\rangle_{123\dots(n+1)} + \beta_i|101\dots 1\rangle_{123\dots(n+1)}), \quad (4)$$

where  $\alpha_i$  and  $\beta_i$  are the input state parameters.

This state is obtained by Alice after performing a XOR operation on the secret available to her at the first iteration with any one of the qubits of the  $n$  qubit GHZ state ( $|GHZ\rangle_n = \frac{1}{\sqrt{2}}[|000\dots 0\rangle + |111\dots 1\rangle]$ ). Alice measures the second qubit in  $\{|0\rangle, |1\rangle\}$  basis and distributes the qubit such that the party who is supposed to reconstruct the secret (say Bob) is given the 1st qubit. In the reconstruction phase all the other parties have to measure their qubits in  $\{|+\rangle, |-\rangle\}$  basis and convey their results to Bob. If Alice wishes to go for further secret sharing the qubits are to be returned back to her by others except Bob. She applies the appropriate unitary transformation to convert them to  $|0\rangle$  state and uses the qubit  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  along with these  $n-1$  qubits to perform a chained XOR. This results in a resource state given by,

$$\xrightarrow{XOR} \frac{1}{\sqrt{2}} \left\{ \underbrace{|000\dots 0\rangle}_n + \underbrace{|100\dots 0\rangle}_n \right\} \quad (5)$$

### SEQUENTIAL SECRET SHARING IN THE PRESENCE OF NOISE

In this section, we consider a more realistic situation where three parties share a three qubit mixed entangled state instead of a three qubit pure entangled state as a resource. Similarly, here also, we start with a pure entangled state  $|\Psi_{in}\rangle$ , initially with all the qubits with Alice. Now Alice keeps the second qubit with herself and sends the remaining qubits (1 & 3) to Charlie and Bob. She sends them through a noisy quantum channel. Since practically no channel is completely noise-free, such an analysis in the absence of noise is imperative. We study our protocol under the effects of both phase damping channel(PDC) and amplitude damping channel(ADC).

#### Transmission of qubits through a PDC

In the first subsection, we study the effects of PDC on the secret sharing fidelity when the qubits are sent through this channel. The action of a PDC are given by the set of three Kraus operators, namely,  $K_0 = \sqrt{1-q}I$ ,  $K_1 = \sqrt{q}|0\rangle\langle 0|$ , and  $K_2 = \sqrt{q}|1\rangle\langle 1|$ ; where  $q(0 \leq q \leq 1)$  is the channel strength [15]. The action of the Kraus operators, describing the PDC, on the two qubits results in a three qubit mixed entangled state,  $\rho_{out}$  are as follows,

$$\rho_{out} = \sum_i \sum_j [(K_i \otimes I \otimes K_j) \rho^{in} (K_i^\dagger \otimes I^\dagger \otimes K_j^\dagger)] \quad (6)$$

where  $i, j \in \{0, 1, 2\}$ . Here the Kraus operators acts on the two qubits sent to Bob and Charlie by Alice. These qubits are the ones which are subjected to environmental interaction and thus undergo phase damping. In the reconstruction phase, Alice measures her qubit in  $\{|0\rangle, |1\rangle\}$  basis and Charlie measures in  $\{|+\rangle, |-\rangle\}$  basis. After these measurements Bob's state collapses to one of the four states,  $\rho_{out}^{a,b}$  (with  $a \in \{0, 1\}$  representing Alice's measurement outcome and  $b \in \{+, -\}$ , representing Charlie's measurement outcome). These four states are given by,

$$\begin{aligned}
\rho_{out}^{0,+} &= \alpha^2 |0\rangle \langle 0| + \beta^2 |1\rangle \langle 1| + \\
&(1-q)^2 \alpha \beta |1\rangle \langle 0| + (1-q)^2 \alpha \beta |0\rangle \langle 1| \\
\rho_{out}^{0,-} &= \alpha^2 |0\rangle \langle 0| + \beta^2 |1\rangle \langle 1| - \\
&(1-q)^2 \alpha \beta |1\rangle \langle 0| - (1-q)^2 \alpha \beta |0\rangle \langle 1| \\
\rho_{out}^{1,+} &= \alpha^2 |1\rangle \langle 1| + \beta^2 |0\rangle \langle 0| + \\
&(1-q)^2 \alpha \beta |1\rangle \langle 0| + (1-q)^2 \alpha \beta |0\rangle \langle 1| \\
\rho_{out}^{1,-} &= \alpha^2 |1\rangle \langle 1| + \beta^2 |0\rangle \langle 0| - \\
&(1-q)^2 \alpha \beta |1\rangle \langle 0| - (1-q)^2 \alpha \beta |0\rangle \langle 1|. \quad (7)
\end{aligned}$$

Since the channel through which the qubits are sent is a noisy channel, the qubit obtained by Bob is no longer the desired qubit but a single qubit mixed state  $\rho_{out}^{a,b}$ . At this point we define the fidelity of quantum secret sharing as the overlap between the original secret and the nearest possible state obtained during the reconstruction phase after optimizing over all possible complex unitaries. The expression for the secret sharing fidelity given by,

$$\text{Maximize}_U \left\langle \psi \left| U \rho_{out}^{a,b} U^\dagger \right| \psi \right\rangle \quad (8)$$

where  $U$  represents complex unitaries.

In our case, after doing optimization over all possible complex unitary matrices, we find that the unitaries that will take the state obtained at Bob's side are the same set of unitaries that are given in TABLE I and the fidelity of secret sharing is given by,

$$F_{PD} = \alpha^4 + 2(1-q)^2 \alpha^2 \beta^2 + \beta^4. \quad (9)$$

The average fidelity obtained after averaging over all input parameter  $\alpha^2$  is given by,

$$\bar{F}_{PD} = 1 - \frac{2q}{3} + \frac{q^2}{3}. \quad (10)$$

In FIG. 1 we plot the average fidelity ( $\bar{F}_{PD}$ ) against the channel strength ( $q$ ). It is evident from the figure itself that when we have no noise in the channel, that is  $q = 0$ , we have  $\bar{F}_{PD} = 1$ . This ensures the fact that in the absence of noise we can always do perfect secret sharing. However, for  $q = 1$  we have the value of the average fidelity to be  $\frac{2}{3}$ . This protocol gives a high secret sharing fidelity of 0.6667 in a situation where we have maximum noise present in the phase damping channel.

### Transmission of qubits through an ADC

In this subsection, we investigate the process of secret sharing when the qubits are sent through amplitude damping channel (ADC).

The action of an ADC are given by the set of two Kraus operators, namely,  $K_0 = |0\rangle \langle 0| + \sqrt{1-p} |1\rangle \langle 1|$ , and  $K_1 = \sqrt{p} |0\rangle \langle 1|$ ; where  $p(0 \leq p \leq 1)$  is the channel strength

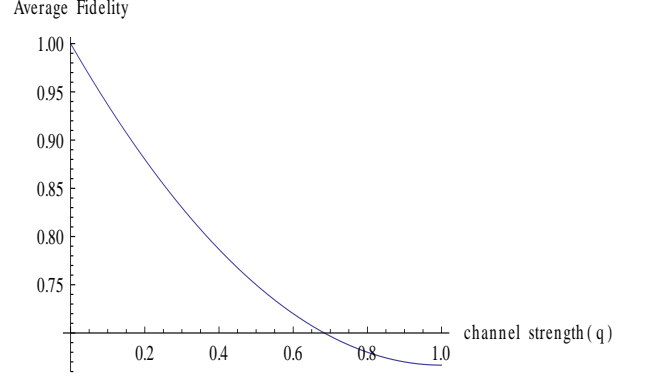


FIG. 1: Variation of Average Fidelity of sequential secret sharing with the PDC parameter( $q$ ).

[15]. The action of the Kraus operators, describing the ADC, on the two qubits (sent to Bob and Charlie) results in a three qubit mixed entangled state,  $\rho_{out}$ .

The four states corresponding to the measurement outcomes are given by,

$$\begin{aligned}
\rho_{out}^{0,+} &= (\alpha^2 + p\beta^2) |0\rangle \langle 0| + (1-p)\beta^2 |1\rangle \langle 1| + \\
&(1-p)\alpha\beta |1\rangle \langle 0| + (1-p)\alpha\beta |0\rangle \langle 1| \\
\rho_{out}^{0,-} &= (\alpha^2 + p\beta^2) |0\rangle \langle 0| + (1-p)\beta^2 |1\rangle \langle 1| - \\
&(1-p)\alpha\beta |1\rangle \langle 0| - (1-p)\alpha\beta |0\rangle \langle 1| \\
\rho_{out}^{1,+} &= (p\alpha^2 + \beta^2) |0\rangle \langle 0| + (1-p)\alpha^2 |1\rangle \langle 1| + \\
&(1-p)\alpha\beta |1\rangle \langle 0| + (1-p)\alpha\beta |0\rangle \langle 1| \\
\rho_{out}^{1,-} &= (p\alpha^2 + \beta^2) |0\rangle \langle 0| + (1-p)\alpha^2 |1\rangle \langle 1| - \\
&(1-p)\alpha\beta |1\rangle \langle 0| - (1-p)\alpha\beta |0\rangle \langle 1| \quad (11)
\end{aligned}$$

Depending on measurement outcome of Alice and Charlie, Bob applies the corresponding unitary transformations according to the ones given by TABLE I.

Proceeding similar to the above case of PDC, the fidelity of quantum secret sharing is obtained by optimizing over all possible complex unitaries given by

$$\bar{F}_{AD} = \alpha^2 + (1-p)\beta^2. \quad (12)$$

Unlike the case of PDC, here we cannot convert all the four  $\rho_{out}^{a,b}$  exactly to  $\rho_{out}^{0,+}$  using unitary operations. However we can convert them pairwise. By applying the unitary operations in TABLE I, we end up with two different fidelity expressions. Both these expressions, when averaged over all possible input states, give rise to the same average fidelity for the protocol. The average fidelity obtained after averaging over all input parameter  $\alpha^2$  is given by

$$\bar{F}_{AD} = 1 - \frac{p}{2} \quad (13)$$

In FIG. 2 we plot the average fidelity ( $\bar{F}_{AD}$ ) against the channel strength ( $p$ ). It is evident from the figure itself that when we have no noise in the channel, that is  $p = 0$  we have  $\bar{F}_{AD} = 1$ , ensuring the fact that in the absence of noise we can always do perfect secret sharing.

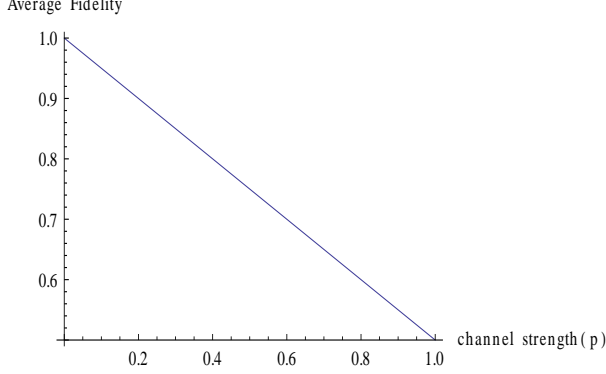


FIG. 2: Variation of Average Fidelity of sequential secret sharing with the ADC parameter( $p$ ).

For both above channels, we observe that in our protocol the fidelity of secret sharing in subsequent iterations remains the same and is independent of the number of iterations. This is because at each and every iteration there is reusability of Charlie's qubit. Though Charlie's qubit is affected by noise and will also get further affected when he sends back his qubit to Alice, this noise is not going to play a part in the subsequent iterations. This is because Alice on getting back the qubit from Charlie measures it in the computational basis  $\{|0\rangle, |1\rangle\}$  and transforms it accordingly to the state  $|0\rangle$  by applying the appropriate unitary transformation.

### IMPROVING THE FIDELITY OF THE SHARED SECRET USING WEAK MEASUREMENTS

In the previous section we have noticed that in a realistic situation the shared qubits are subjected to decoherence due to the presence of noise. This environmental interaction results in inevitable loss of fidelity of obtaining the shared secret. The reconstructed secret under noise becomes a mixed state, and under certain conditions the average fidelity drops to  $\frac{1}{2}$ . It then becomes of no more use than what can be obtained by employing random guess. Thus, there arises an exigency to improve the fidelity of reconstructing the shared secret.

The authors in the references [10, 11, 12, 13], have shown that one can reduce the effect of amplitude damping decoherence with the help of weak measurement and reverse quantum measurement (WMRQM) [11]. Recently the authors in [14] show how to improve the fidelity of teleportation through noisy channel with the

aid of weak measurements. In this section, we show how to improve the fidelity of the shared secret in the protocol of sequential quantum secret sharing under the influence of ADC with the help of weak measurements and post-selection. We find that in the case of PDC since both the qubit states  $|0\rangle$  and  $|1\rangle$  get affected by decoherence, unlike ADC where  $|0\rangle$  state remains unaltered, this method of reverse weak measurement and post-selection cannot be employed to improve the fidelity of the shared secret.

In this protocol we apply weak measurements and its reversal, in two stages: one before and other after the decoherence acts on the system. After preparing the state represented in Eq. 2, Alice makes a weak measurement [11, 14] of strength  $s_i$  on the  $i^{th}$  qubit where  $i = \{1, 3\}$ . The weak measurement here is ensured by reducing the sensitivity of the detector. On one hand the detector clicks with probability  $s_i$  if the input qubit is in state  $|1\rangle_i$  and subsequently the protocol fails since the input state collapses on  $|1\rangle_i$  in an irreversible way. On the other hand the detector never clicks if its in state  $|0\rangle_i$  but it partially biases the input state towards  $|0\rangle_i$  which remains unaffected by the damping interaction given by Eq. 6. The measurement operator corresponding to the detection and non-detection of the qubits are respectively given by,

$$M_{q,1} = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{s_q} \end{pmatrix} \quad (14)$$

which is irreversible since it doesn't possess an inverse, and

$$M_{q,0} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-s_q} \end{pmatrix} \quad (15)$$

which is reversible as it has an inverse. Here  $M_{q,0}^\dagger M_{q,0} + M_{q,1}^\dagger M_{q,1} = I$  and  $q = \{1, 3\}$  represent the qubit on which the measurement is being performed. Alice makes this weak measurement on 1st and 3rd qubit and sends them to Charlie and Bob respectively.

If  $\rho_{in}$  be the density matrix corresponding to the pure state  $|\Psi_{in}\rangle$  in Eq. 2, then the output state after the measurement is a mixed state and is denoted by  $\rho^{WW}$

$$\rho^{WW} = (M_{1,0} \otimes I \otimes M_{3,0}) \rho_{in} (M_{1,0}^\dagger \otimes I^\dagger \otimes M_{3,0}^\dagger). \quad (16)$$

For our convenience, we assume the input state parameters,  $\alpha^2 = k$  and  $\beta^2 = 1 - k$ . The success probability of the measurement or in other words the detector's inefficiency is given by,  $SP_1 = Tr[\rho^{WW}] = \frac{1}{2}(1 + \bar{s})(1 - \bar{k}s)$ , where  $\bar{s} = (1 - s)$  and  $\bar{k} = (1 - k)$ .

Alice then sends both the qubits (1 and 3) to Charlie and Bob through the ADC where they suffer decoherence due to interaction with the environment. Owing to this effect the mixed state  $\rho^{WW}$  takes the form,

$$\rho^{DD} = \sum_i \sum_j [(K_i \otimes I \otimes K_j) \rho^{WW} (K_i^\dagger \otimes I^\dagger \otimes K_j^\dagger)] \quad (17)$$

where  $i, j = \{0, 1\}$  in the case of ADC.

Lastly, Bob and Charlie perform the reverse quantum measurement [11, 14]  $N_{z,0}$  (corresponding to  $M_{q,0}$  in Eq. 11 on the qubits received from Alice after suffering decoherence. The operators for reverse weak measurements are given by,

$$N_{z,0} = \begin{pmatrix} \sqrt{1-r_z} & 0 \\ 0 & 1 \end{pmatrix} \quad (18)$$

where  $r$  denotes the reverse quantum measurement strength and  $z = \{1, 3\}$  denotes the qubit on which measurement is being performed.

The output state, after the measurement, is again a mixed state and is denoted by  $\rho^{RR}$  and is given by,

$$\rho^{RR} = (N_{1,0} \otimes I \otimes N_{3,0}) \rho^{DD} (N_{1,0}^\dagger \otimes I^\dagger \otimes N_{3,0}^\dagger) \quad (19)$$

In this case, the overall success probability,

$$SP_2 = \frac{1}{2} (k\bar{r} - \bar{k}\delta\bar{s})(2 - (1+p)r + \delta s) = \text{Tr} [\rho^{RR}] \quad (20)$$

where  $\delta = (pr-1)$ ,  $\bar{r} = (1-r)$ ,  $\bar{s} = (1-s)$  and  $\bar{k} = (1-k)$ .

For simplicity, here we assume the measurement strengths to be uniform,  $s_1 = s_3 = s$  and  $r_1 = r_3 = r$ .

To reconstruct the secret at Bob's end, Alice measures her qubit in computational basis  $\{|0\rangle, |1\rangle\}$  and Charlie measures in horizontal basis  $\{|+\rangle, |-\rangle\}$ . After these measurements Bob's state collapses to one of the four states,  $\rho_{out}^{a,c}$ , with  $a \in \{0, 1\}$  representing Alice's measurement outcomes and  $c \in \{+, -\}$ , representing Charlie's measurement outcomes. Alice and Charlie send their measurement outcome to Bob over classical channel. Just as before depending on these results, Bob applies the optimal unitary transformations (same as the ones given by TABLE I), to reconstruct the secret.

We illustrate two cases, one when the Alice's measurement outcome is  $|0\rangle$  and the other when its  $|1\rangle$ , since the expression of the fidelity of the shared secret obtained in these two cases are not the identical, similar to the situation when no weak measurement is performed.

*Case I.* When Alice's measurement outcome is  $|0\rangle$ , then the output density matrix,  $\rho_{out}^{0,+}$ , is as follows,

$$\begin{pmatrix} \frac{(-1+r)((-1+r)\alpha^2 + p(-1+s)^2\beta^2\delta)}{\eta} & -\frac{j\alpha\beta}{\eta} \\ -\frac{j\alpha\beta}{\eta} & \frac{(-1+p)(-1+s)^2\beta^2\delta}{\eta} \end{pmatrix} \quad (21)$$

where  $\delta = (pr-1)$ ,  $\eta = (r-1)^2\alpha^2 + (pr-1)^2(s-1)^2\beta^2$  and  $(p-1)(r-1)(s-1) = j$ .

The fidelity of the shared secret ( $F_0^{WW}$ ), is given by,

$$F_0^{WW} = \frac{k^2\bar{r}^2 - \bar{k}^2\bar{s}^2\bar{p}\delta + k\bar{k}\bar{s}\bar{r}(2 - (1+s)p - \bar{s}p^2r)}{k\bar{r}^2 + \bar{k}\bar{s}^2\delta^2} \quad (22)$$

where  $\delta = (pr-1)$ ,  $\bar{r} = (1-r)$ ,  $\bar{p} = (1-p)$ ,  $\bar{k} = (1-k) = \beta^2$  and  $\bar{s} = (1-s)$ .

In this protocol, the role of forward weak measurement is to project the input state towards  $|0\rangle$ , which is unaffected by the environmental interaction. One can think of this as a map from  $|1\rangle$  to  $|0\rangle$ , which is reversible. Since we have use a map from  $|1\rangle \rightarrow |0\rangle$  at beginning so we need to again use a reverse map i.e., from  $|0\rangle \rightarrow |1\rangle$  later. Moreover as the state is suffers the decoherence in its transit, we use the optimal strength of reverse quantum measurement which is a function of noise. Thus its crucial that the optimization should always be done on reverse quantum measurement strength ( $r$ ) and not on forward one ( $s$ ).

To achieve the objective of the protocol one needs to choose the proper strengths of the weak measurement. The optimum reverse measurement strength  $r_{opt}$  which maximally protects the fidelity of the shared secret ( $F_0^{WW}$ ) is obtained by maximizing Eq. 22 with respect to  $r$ . The optimum reverse measurement strength, in this case, is given by

$$r_{opt} = -\sqrt{-\frac{k\bar{p}^2\bar{s}^2}{(k(p^2\bar{s}^2 - 1) - p^2\bar{s}^2)f^2}} + \frac{1 + (2k-1)s}{f}, \quad (23)$$

where  $f = p + 2k(1-p\bar{s}) - ps$  and the range of optimality is given by the following condition,  $0 < p < 1$  &  $0 < s < 1$  &  $\left(\frac{-p+ps}{-2-2p+2ps} < k < \frac{-1+s}{-4+2s} \parallel \frac{-1+s}{-4+2s} < k < 1\right)$ .

Substituting this expression for  $r_{opt}$ , given by Eq. 23, in

Eq. 22, in place of  $r$ , one can get the expression to obtain

optimal fidelity of the shared secret,  $F_{opt}^0$ . Hence, by averaging over the allowed range of input state parameter  $k$  (as given above), the average optimal fidelity ( $\bar{F}_{opt}^0$ ) is

$$\bar{F}_{opt}^0 = \frac{1}{8uv^2} \{ (8 - p\bar{s})(p\bar{s} + 2)(4 - 3p\bar{s})u \} + \frac{1}{8uv^2} \left\{ 2p^2\bar{s}^2v^2 \left( \ln \left[ p\bar{s} \left( 1 - u + p\bar{s} \left( 1 + u - 2\sqrt{\frac{2}{v} - 1} \right) + 2p^2\bar{s}^2\sqrt{\frac{2}{v} - 1} \right) \right] - \ln [(2 - p^2\bar{s}^2 - 2u)v] \right) \right\} \quad (24)$$

for  $0 < p < 1$  &  $0 < s < 1$ . Here,  $u = \sqrt{1 - p^2\bar{s}^2}$  and  $v = 1 + p - ps$ .

Thus, for a given value of  $p$  (or decoherence channel strength), one can always choose a value of weak measurement strength( $s$ ) within the permitted range, given by the above condition, to calculate the average optimal fidelity,  $\bar{F}_{opt}^0$ .

In FIG. 3, we compare how  $\bar{F}_{opt}^0$  is protected by WM-RQM even when very strong decoherence strength is applied. In this case we find that the average optimal fidelity ( $\bar{F}_{opt}^0$ ) stays close to  $\frac{3}{5}$  for very high decoherence strength even at  $s = 0$ . This is a noticeable improvement over the case when no such WM-RQM is employed, the average fidelity is  $\frac{1}{2}$  when the decoherence strength is very high. This clearly illustrates that the role of reverse quantum measurement ( $r$ ) in protecting the fidelity of the shared secret is more pronounced than the forward one.

It is interesting to note that for obtaining very high fidelity of the shared secret using WM-RQM, at high values of decoherence strength ( $p$ ) as shown in FIG. 3, one always has to employ very strong weak measurement ( $s$ ). Intriguingly, here we observe that for very low decoherence strength ( $p$ ) and very low weak measurement strength ( $s$ ),  $\bar{F}_{opt}^0$  obtained using WM-RQM is slightly lower than  $\bar{F}_{AD}$  obtained when no such weak measurement is employed.

Substituting the value of  $r_{opt}$ , given by Eq. 23, in Eq. 20 for  $r$ , one can get the required expression and calculate the corresponding average success probability of the process by then integrating over the prescribed range of input state parameter. We observe that as  $s \rightarrow 1$  the success probability of the process tends to zero (becomes negligibly small) which coheres with results observed by the authors in [14]. Next, In FIG. 4, we illustrate how the average success probability of the process decays rapidly with increase in weak measurement strength ( $s$ ). Also comparing FIG. 4 with FIG. 3, we note that there is a trade off between the fidelity and the success probability of the process.

given by,

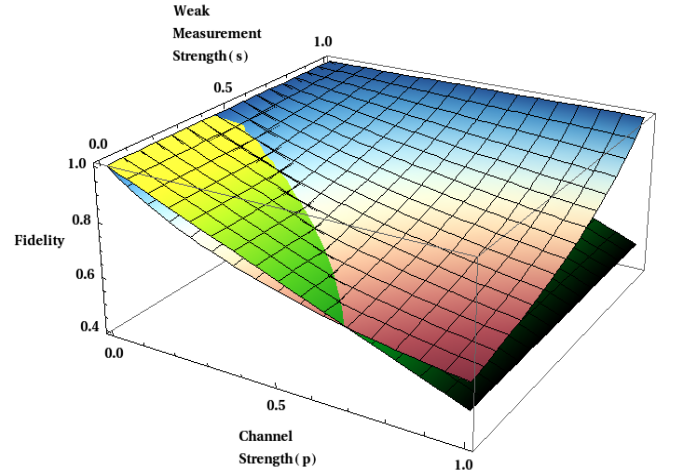


FIG. 3: The green surface represents average fidelity ( $\bar{F}_{AD}$ ) in the case when no WM-RQM is employed (the decrease in fidelity is indicated by transition of light to dark green color). The blue-red surface represents the average optimal fidelity ( $\bar{F}_{opt}^0$ ) of the shared secret when WM-RQM is employed (the decrease in fidelity is indicated by transition of blue to red color).

*Case II.* When Alice's measurement outcome is  $|1\rangle$ , the output density matrix,  $\rho_{out}^{1,+}$  after applying the unitary transformation  $\sigma_x$ , is given by,

$$\frac{1}{1 - pr} \begin{pmatrix} \bar{p}\alpha^2 & \bar{p}\alpha\beta \\ \bar{p}\alpha\beta & 1 - pr + \bar{p}\alpha^2 \end{pmatrix} \quad (25)$$

where  $\bar{p} = (1 - p)$ .

For our convenience, we again assume that the input state parameters,  $\alpha^2 = k$  and  $\beta^2 = 1 - k$ . In this case, the final fidelity of the shared secret ( $F_1^{WW}$ ), is given by,

$$F_1^{WW} = \frac{p(k + r - kr) - 1}{pr - 1} \quad (26)$$

Interestingly, in  $\rho_{out}^{1,+}$  the strength of weak measure-



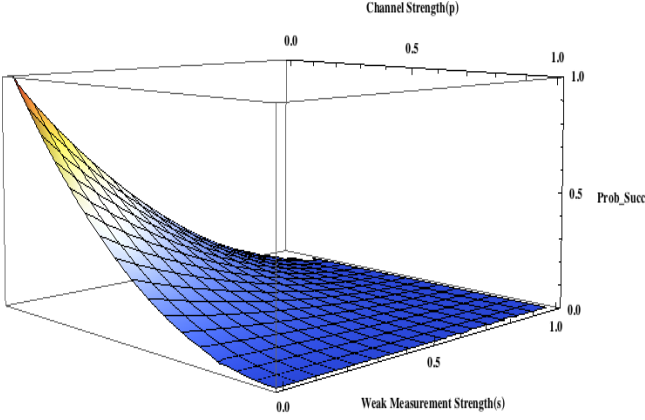


FIG. 4: The surface represents the average success probability (Prob\_Succ) of employing WMRQM (the decrease in average success probability is indicated by transition of red to blue color).

ment parameter ( $s$ ) vanishes and the reverse quantum measurement parameter ( $r$ ) is the only parameter left to protect the fidelity. To achieve the objective of the protocol one needs to choose proper strengths of weak measurement. The optimum reverse measurement strength  $r$  which maximally protects the fidelity of the shared of secret ( $F_1^{WW}$ ) is obtained putting  $r = 1$ . With this substitution in Eq. 26 the optimal fidelity becomes 1, but the success probability corresponding to this case reduces to negligibly small value. The average fidelity ( $\bar{F}^1$ ) obtained by integrating Eq. 26 over the allowed range of input state parameter, is given by,

$$\bar{F}^1 = \frac{p + pr - 2}{2pr - 2} \quad (27)$$

for  $0 < p < 1$  &  $0 < s < 1$ . To analyze what values of reverse measurement strength ( $r$ ) will give better success probabilities as well as increase the average fidelity of the shared secret we plot  $\bar{F}^1$ , varying with decoherence strength ( $p$ ) and strength of reverse measurement ( $r$ ) in FIG. 5.

## CONCLUSIONS

In a nutshell, in this work we have given a protocol for sequential secret sharing of quantum information. Initially we have given the protocol for three parties and then we have generalized it for ( $n > 3$ ) parties. Not only that, we have further considered a much more realistic situation, where we have shared the qubits through two kinds of noisy channels, namely the phase damping channel (PDC) and the amplitude damping channel (ADC). When we carry out the sequential secret sharing in the presence of noise we observe that the fidelity of secret sharing at the  $k^{th}$  iteration is independent of the effect of

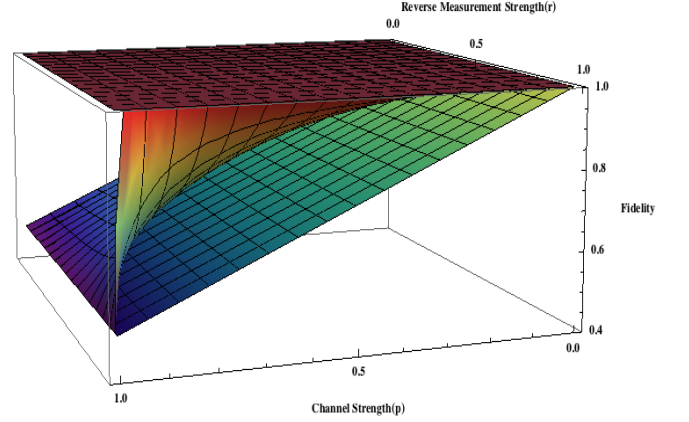


FIG. 5: The dark red flat plain on the top represents the surface which describes the case of optimal fidelity when  $r = 1$ . The rainbow colored surface, in the middle, represents the average fidelity ( $\bar{F}^1$ ) of the shared secret when WMRQM is employed (the decrease in fidelity is indicated by transition of red to violet color). The greenish yellow surface, at the bottom, represents average fidelity ( $\bar{F}_{AD}$ ) in the case when no WMRQM is employed (the decrease in fidelity is indicated by transition of yellow to green color).

noise at the  $(k - 1)^{th}$  iteration. In case of PDC, the average fidelity ranges from 0.67 to 1, whereas in case of ADC we have observed that the average fidelity ranges from 0.5 to 1. In case of ADC, for some value of the channel parameter the average fidelity drops down to 0.5, which is no better than the random guess of the qubits. In order to enhance the fidelity of secret sharing in ADC, we have applied technique of weak measurement. By applying both forward and reverse weak measurement before and after the sharing of the qubits respectively, we have enhanced the average fidelity of secret sharing depending upon the strength parameter and success probability of the measurements.

*Acknowledgment:* Authors gratefully acknowledge Dr. K. Srinathan, Mr. T. Pramanik, Mr. V. Chiranjeevi, Mr. S. Sazim and Mr. N. Ganguly for having many valuable and illuminating discussions.

- 
- [1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
  - [2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993); D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature **390**, 575 (1997).
  - [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
  - [4] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999); R. Cleve, D. Gottesman, and H-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
  - [5] R. Cleve et.al, Phys.Rev.Lett. **83** 648-651 (1999).
  - [6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**,



- 162 (1999).
- [7] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).
  - [8] S. Bagherinezhad, and V. Karimipour, Phys. Rev. A **67**, 044302 (2003).
  - [9] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
  - [10] M. Koashi and M. Ueda, Phys. Rev. Lett. **82**, 2598 (1999).
  - [11] Y.S. Kim, Y.W. Cho, Y.S. Ra, Y.H. Kim, Opt. Express **17**, 11978 (2009).
  - [12] J.C. Lee, Y.C. Jeong, Y.S. Kim, and Y.H. Kim Opt. Express **19**, 16309 (2011).
  - [13] Y.S. Kim, Y.C. Lee, O. Kwon and Y.H. Kim, Nat. Phys. **8**, 117 (2012).
  - [14] T. Pramanik, and A.S. Majumdar, Phys. Lett. A **377**, 3209-3215 (2013).
  - [15] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2002).
  - [16] Y. Aharonov, Z.D. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351-1354 (1988); I.M. Duck, P.M. Stevenson, and E.C.G. Sudarshan, Phys. Rev. D **40** 2112 (1989).
  - [17] G. Gordon, and G. Rigolin, Phys. Rev. A
  - [18] S. B. Zheng, Phys. Rev. A **74**, 054303 (2006).
  - [19] A. Keet, B. Fortescue, D. Markham, B. C. Sanders, Phys. Rev. A **82**, 062315 (2010)
  - [20] D. Markham, B.C. Sanders, Physical Review A **78**, 042309 (2008).
  - [21] Q. Li, W. H. Chan, and D-Y Long, Phys. Rev. A **82**, 022303 (2010).
  - [22] S. Adhikari, Quantum secret sharing with two qubit bipartite mixed states, arXiv:1011.2868.
  - [23] S. Adhikari, I. Chakrabarty, P. Agrawal, Quantum Information and Computation, **12**, 0253 (2012).
  - [24] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
  - [25] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
  - [26] C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Fortschritte der Physik **54**, 831 (2006).
  - [27] J. Bogdanski, N. Rafei, and M. Bourennane, Phys. Rev. A **78**, 062307 (2008).
  - [28] S.k. Sazim, C. Vanarasa, I. Chakrabarty, and K. Srinathan, arXiv:1311.5378.
  - [29] S.k. Sazim and I. Chakrabarty, Eur. Phys. J. D **67**, 8 (2013) 174.